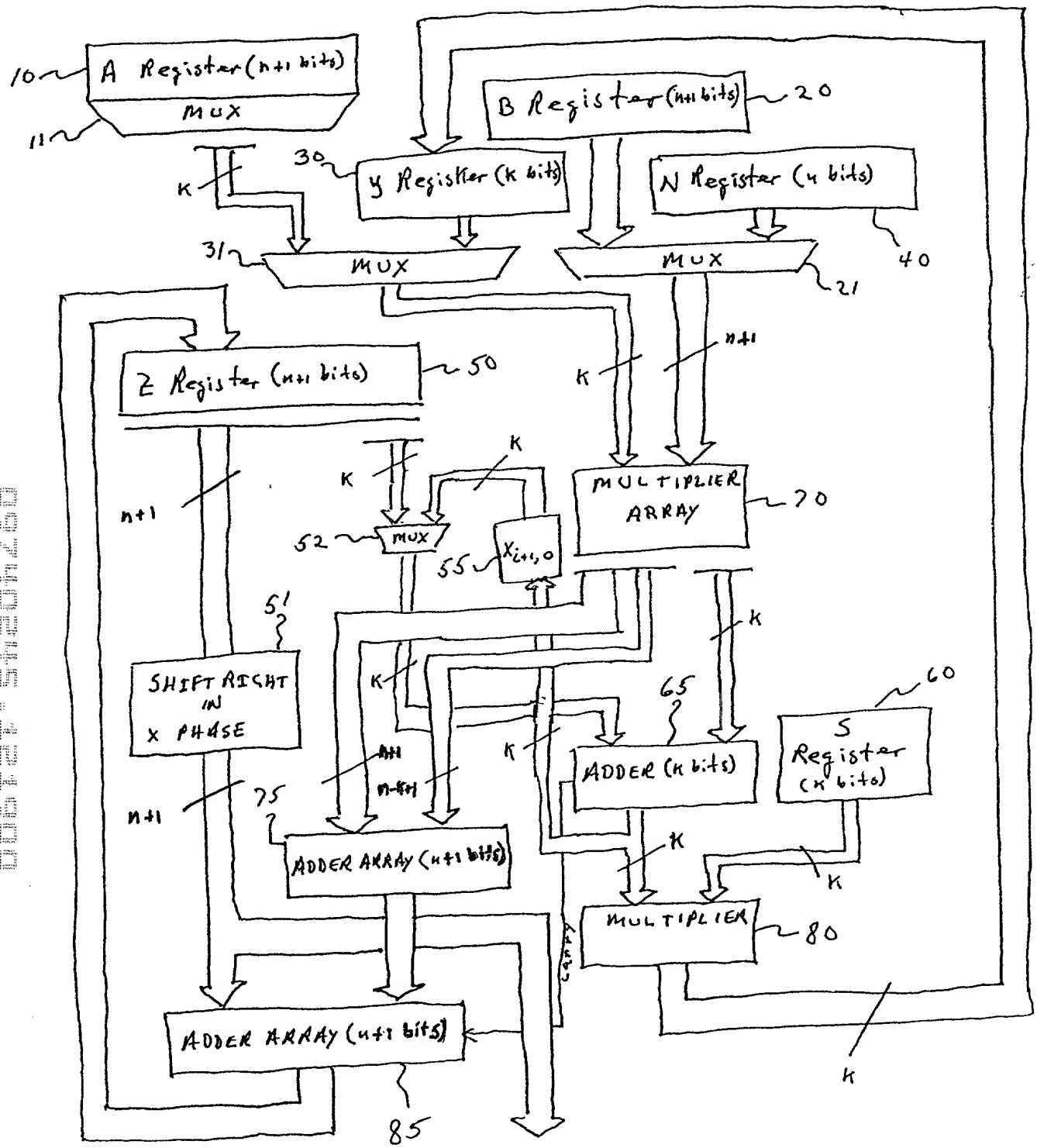
A Register (n+1 bits)
MUX
B Register (n+1 bits)
y Register (k bits)
N Register (n bits)
MUX
MUX
Z Register (n+1 bits)
MULTIPLIER ARRAY
MUX
SHIFT RIGHT IN X PHASE
ADDER (k bits)
S Register (k bits)
ADDER ARRAY (n+1 bits)
MULTIPLIER
ADDER ARRAY (n+1 bits)
10
11
20
30
31
40
21
50
51
52
55
60
65
70
75
80
85
n+1
k

Figure 1

POU 92000 088US 1

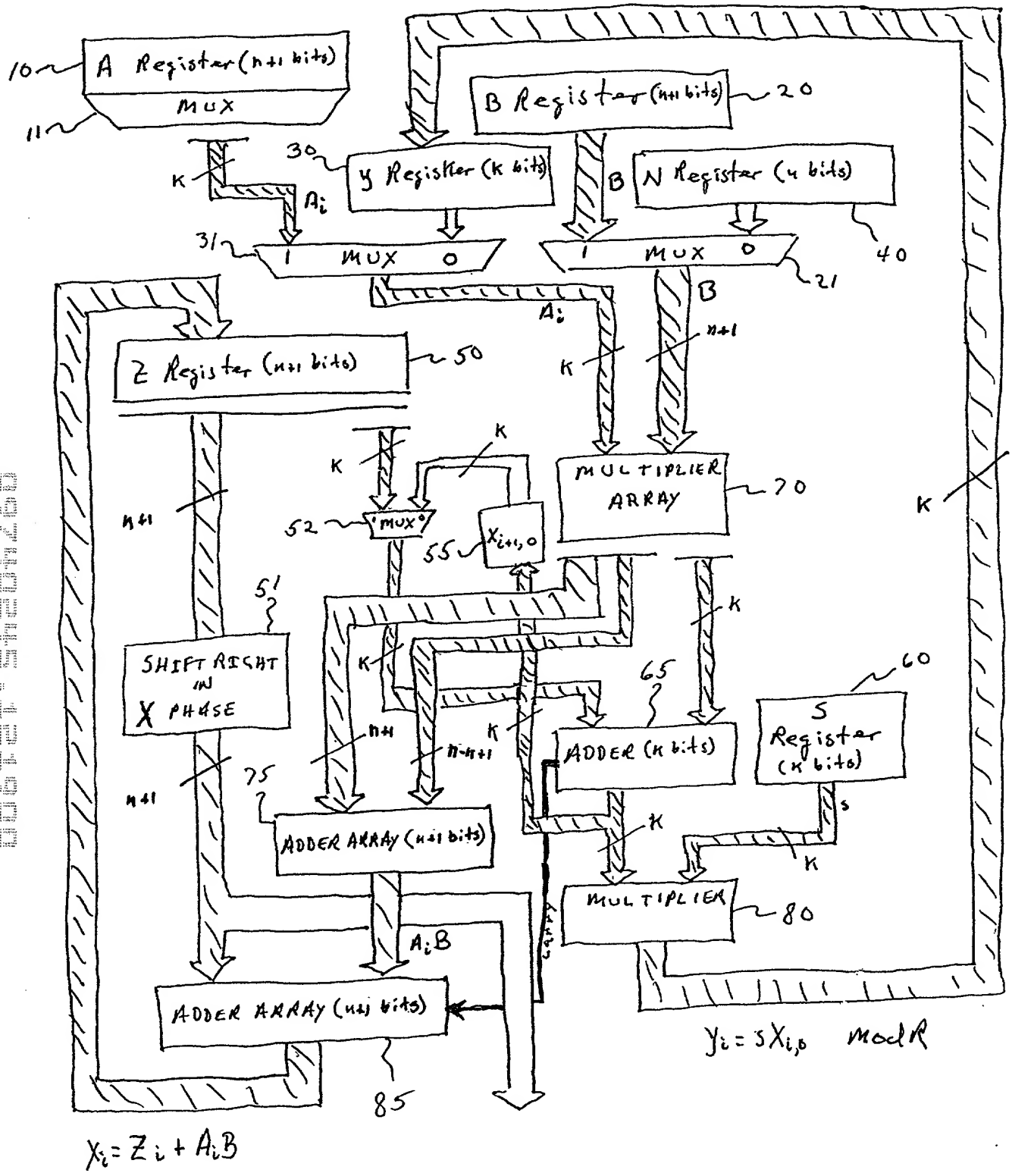

Figure 2

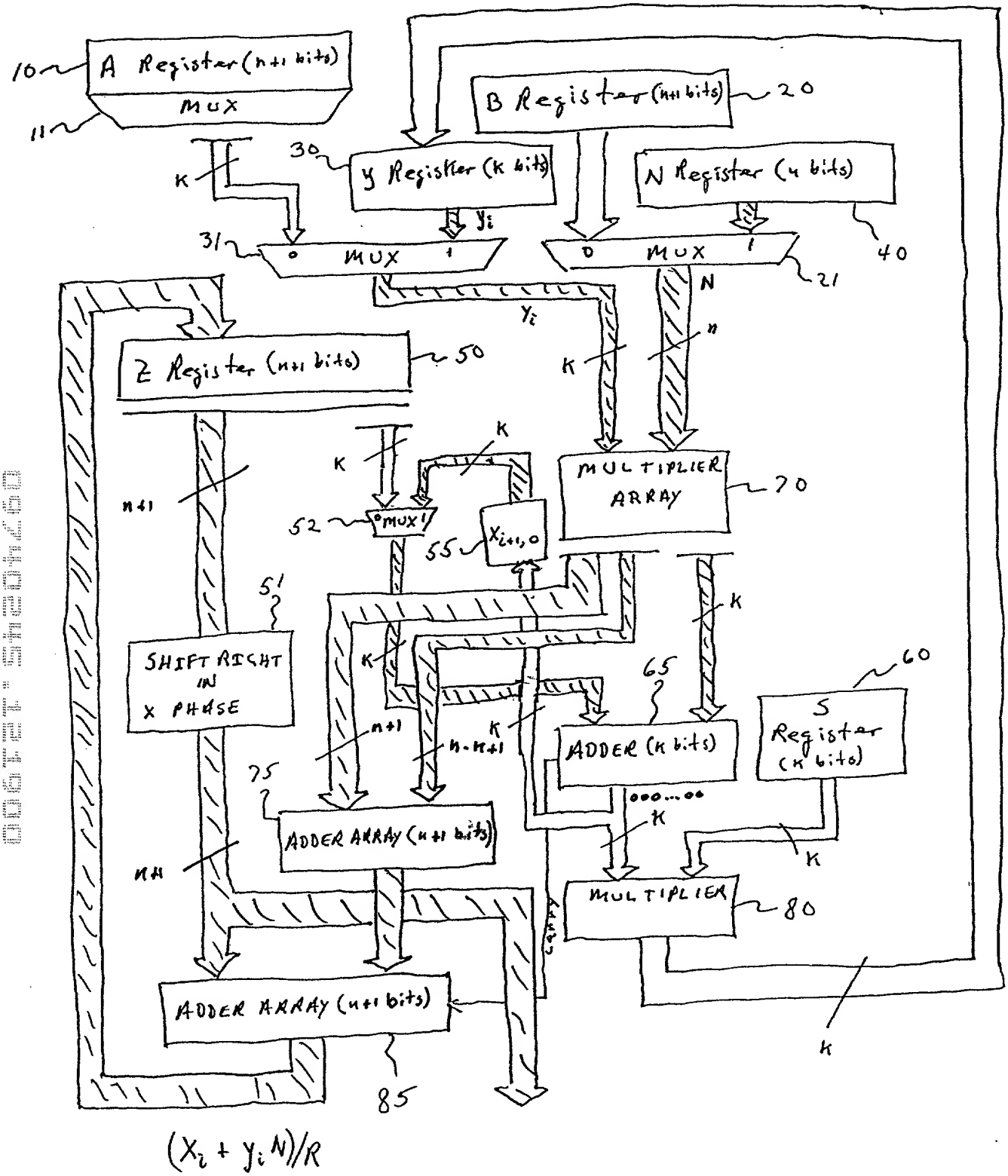

Figure 3

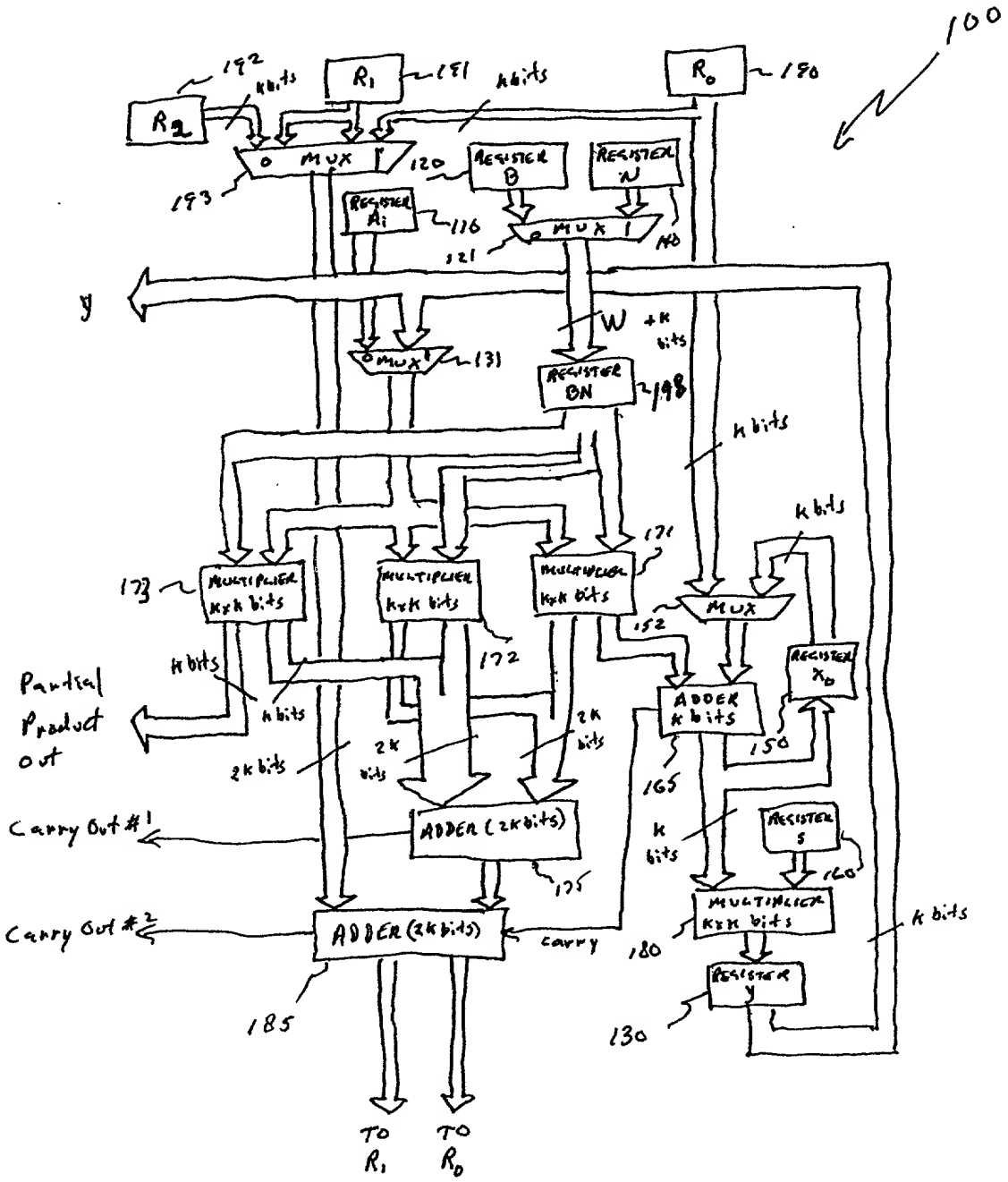

Figure 4

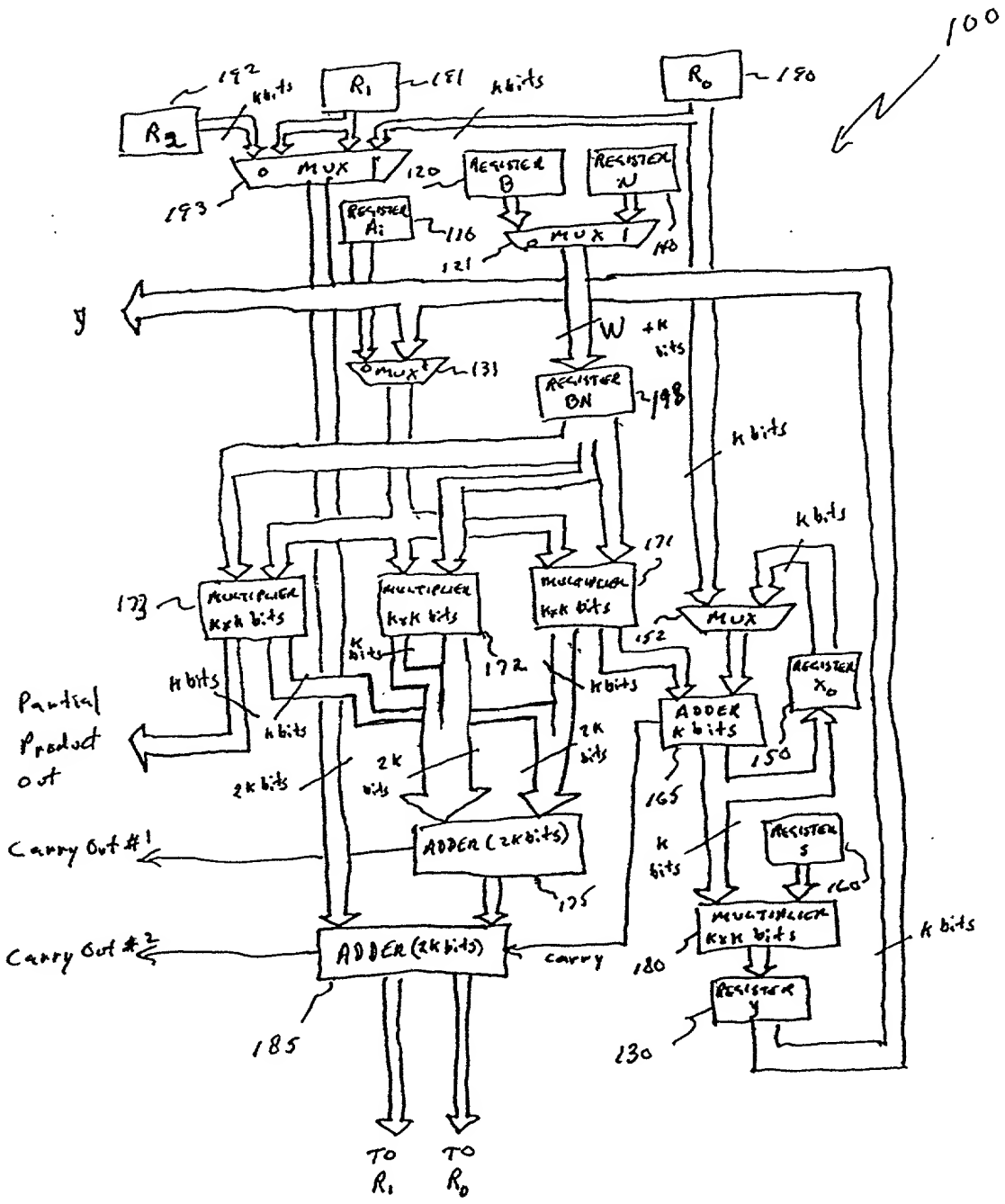
100
R_2
192
k bits
R_1
191
k bits
R_0
190
MUX
120
193
REGISTER B
REGISTER N
REGISTER A_i
116
MUX
121
110
y
W
+k bits
MUX
131
REGISTER BN
198
k bits
k bits
171
MULTIPLIER k x k bits
MULTIPLIER k x k bits
MULTIPLIER k x k bits
MUX
152
173
k bits
172
k bits
k bits
Partial Product out
k bits
2k bits
2k bits
2k bits
ADDER k bits
150
REGISTER X_0
165
k bits
REGISTER S
160
ADDER (2k bits)
175
Carry Out #1
Carry Out #2
ADDER (2k bits)
carry
MULTIPLIER k x k bits
k bits
180
REGISTER Y
185
130
TO R_1
TO R_0

Figure 4A

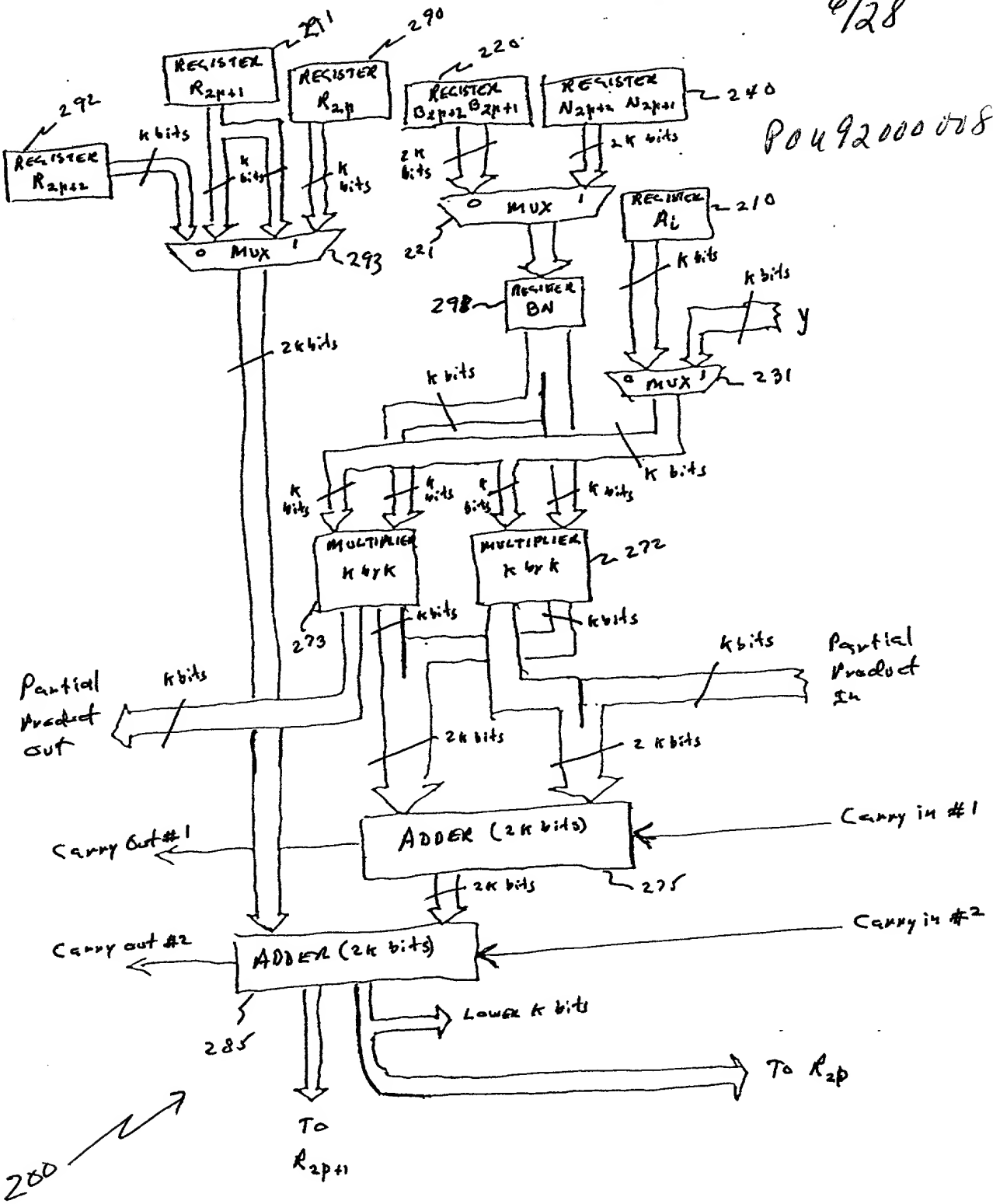

Figure 5

POU920000088US1

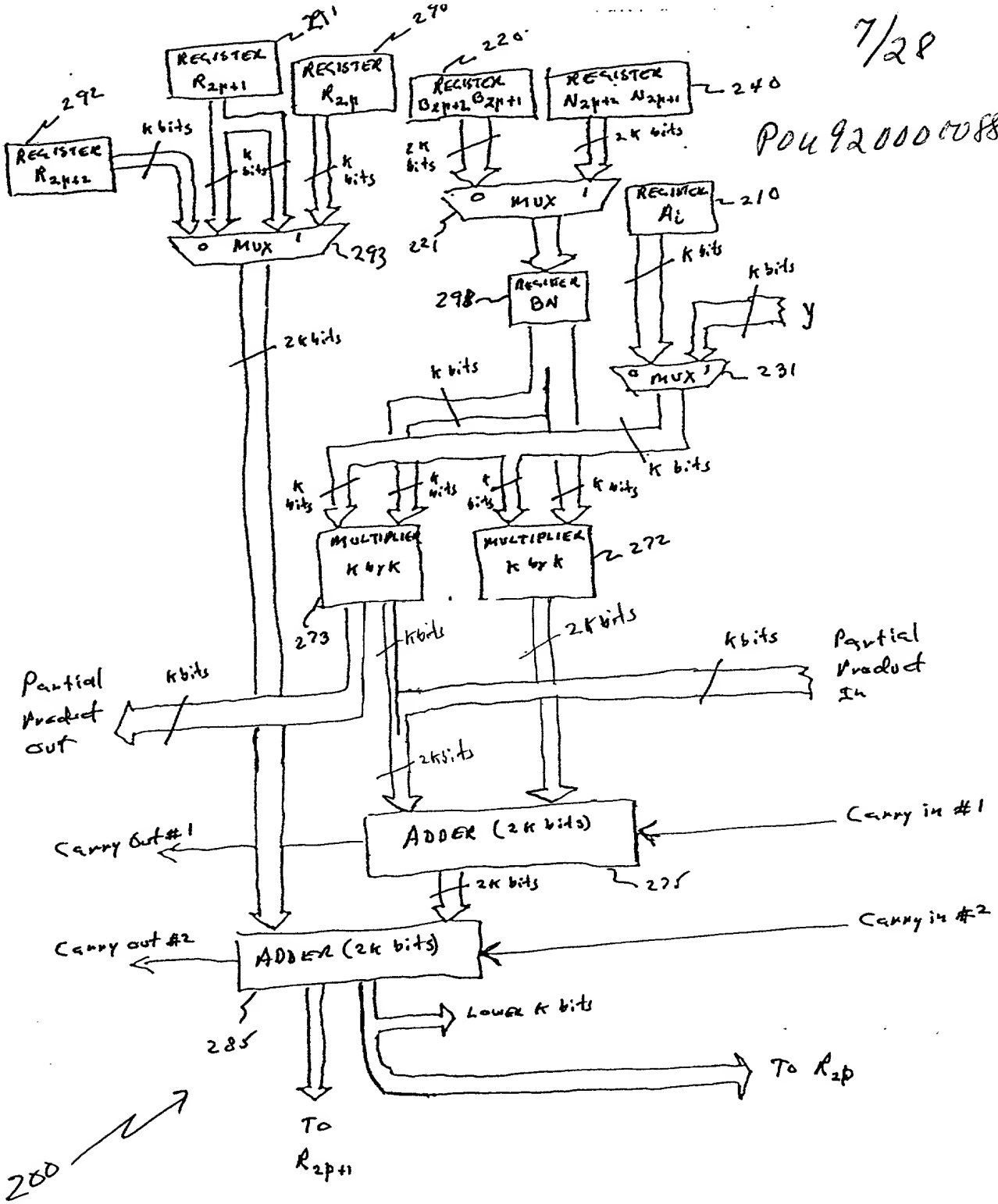

Figure 5A

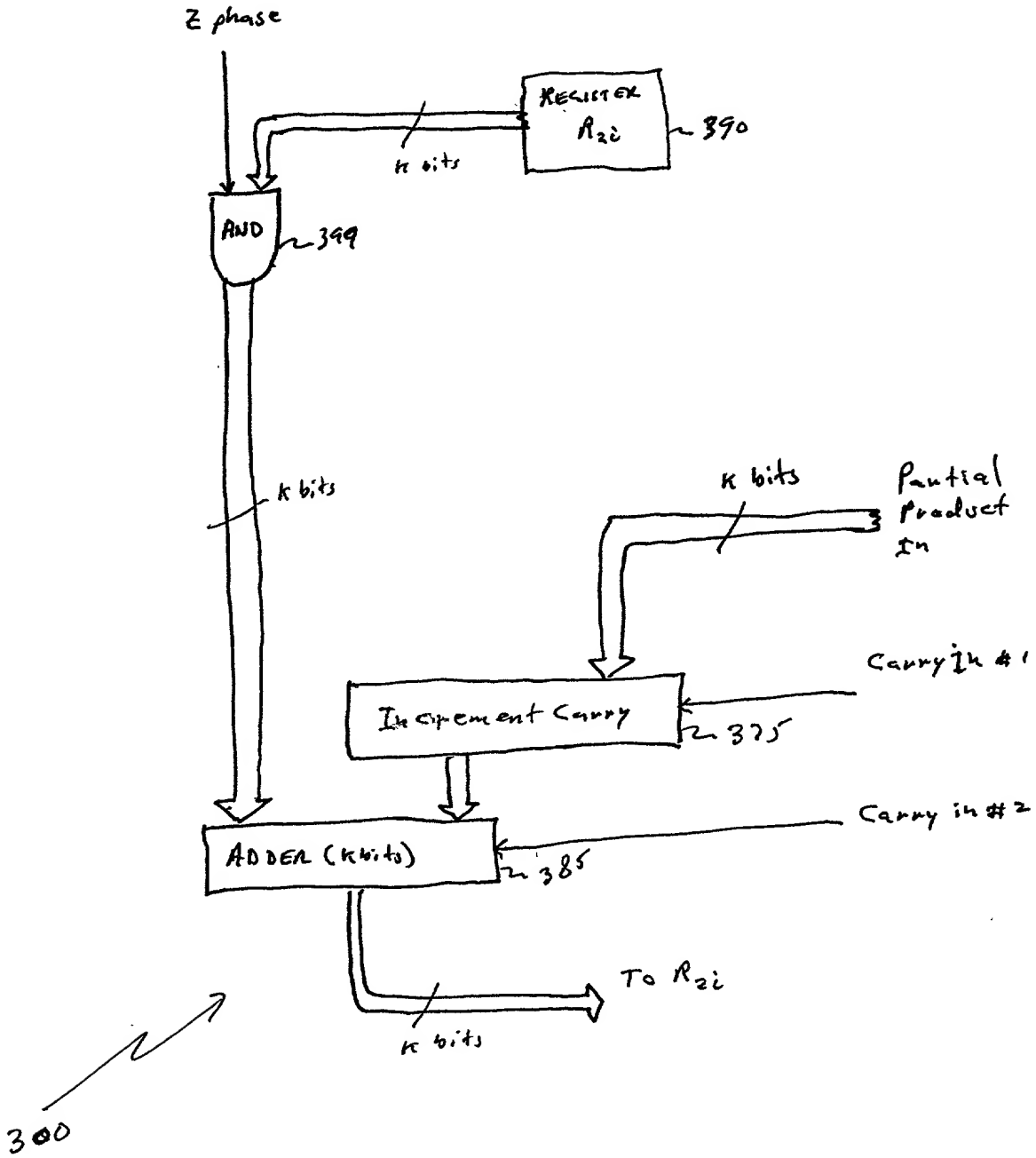

Figure 6

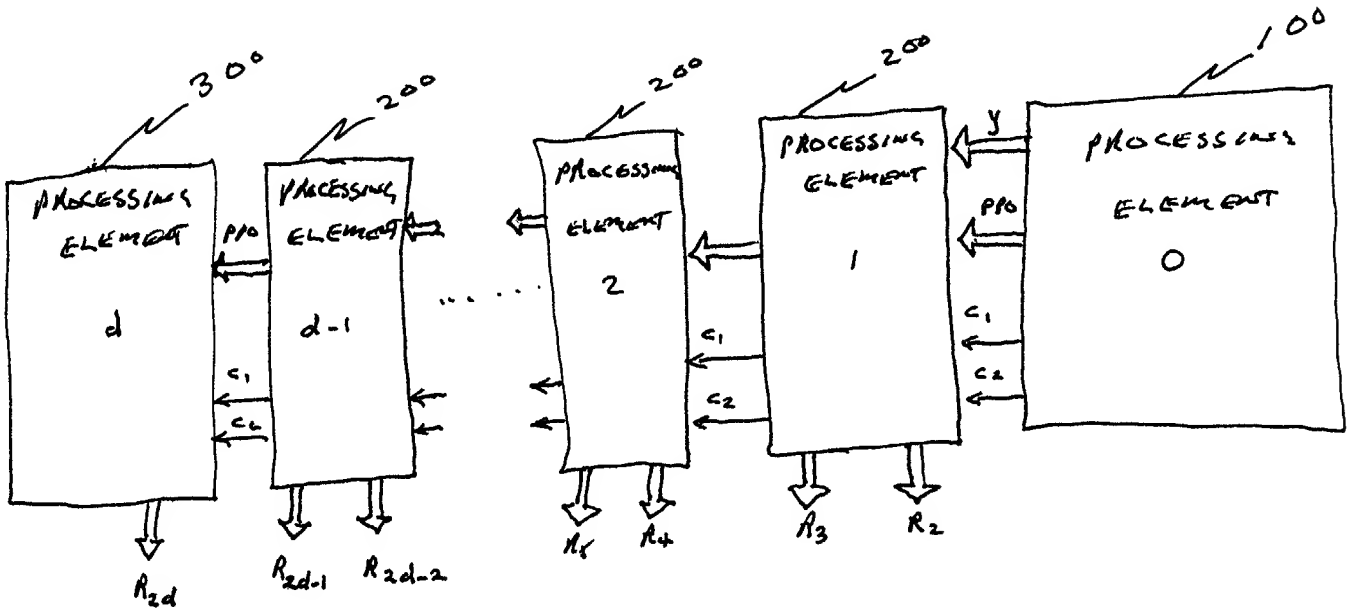

Figure 7

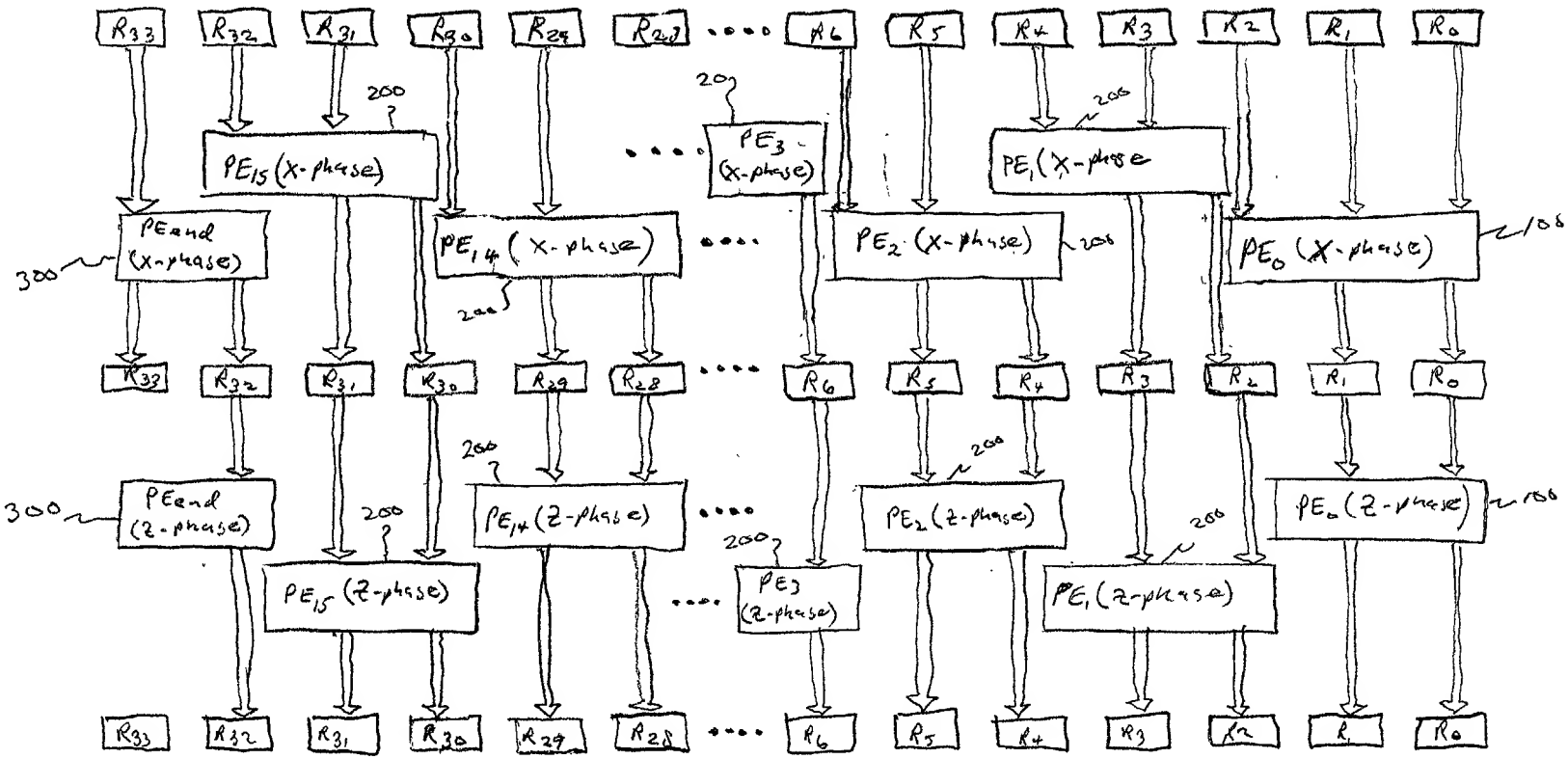
R_{33} R_{32} R_{31} R_{30} R_{29} R_{28} .... R_6 R_5 R_4 R_3 R_2 R_1 R_0
200
PE_{15} (X-phase)
PE_3 (X-phase)
PE_1 (X-phase
300
PEend (X-phase)
PE_{14} (X-phase)
PE_2 (X-phase)
106
PE_0 (X-phase)
PEend (Z-phase)
PE_{14} (Z-phase)
PE_2 (Z-phase)
PE_0 (Z-phase)
PE_{15} (Z-phase)
PE_3 (Z-phase)
PE_1 (Z-phase)

Figure 8

Pau 92000 088US1

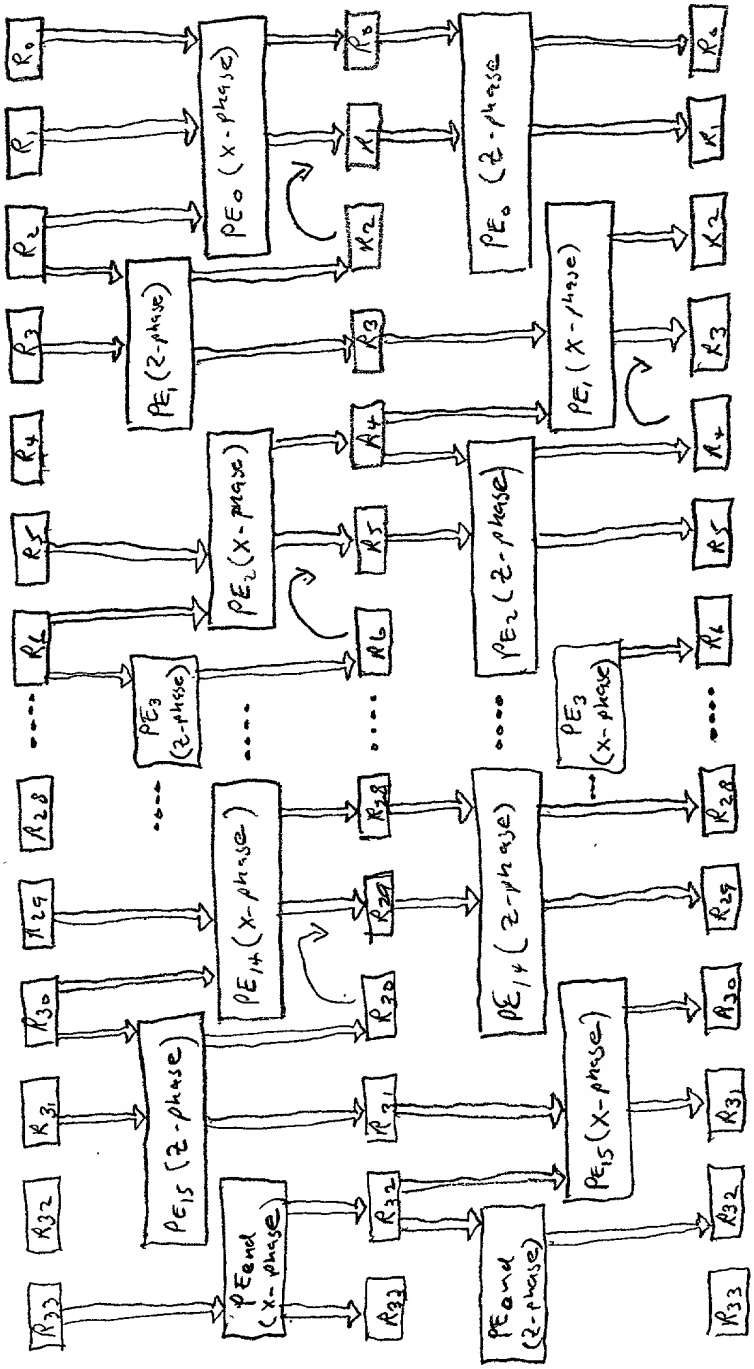

Figure 9

PCT/US92/00088451

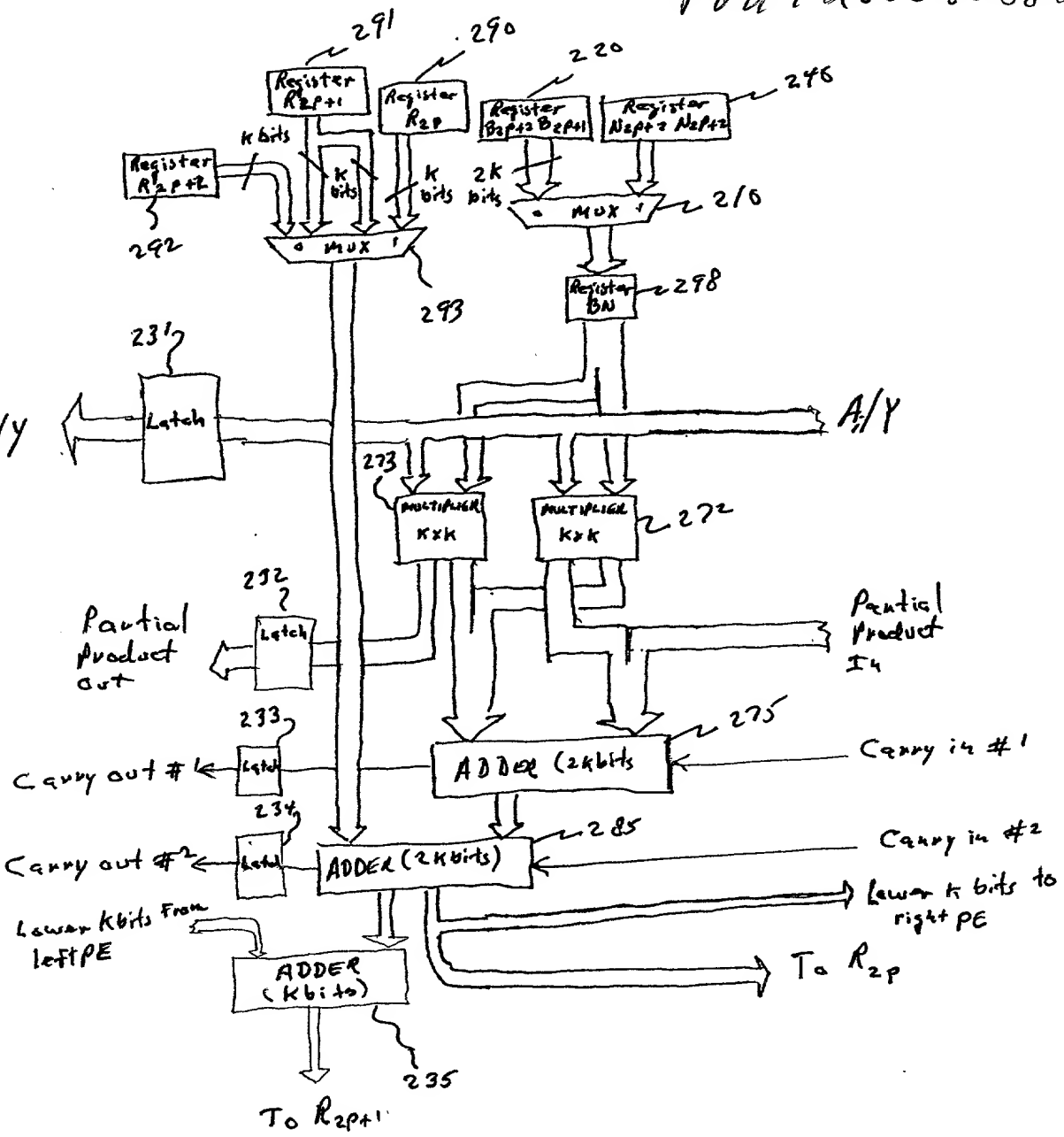

Figure 10

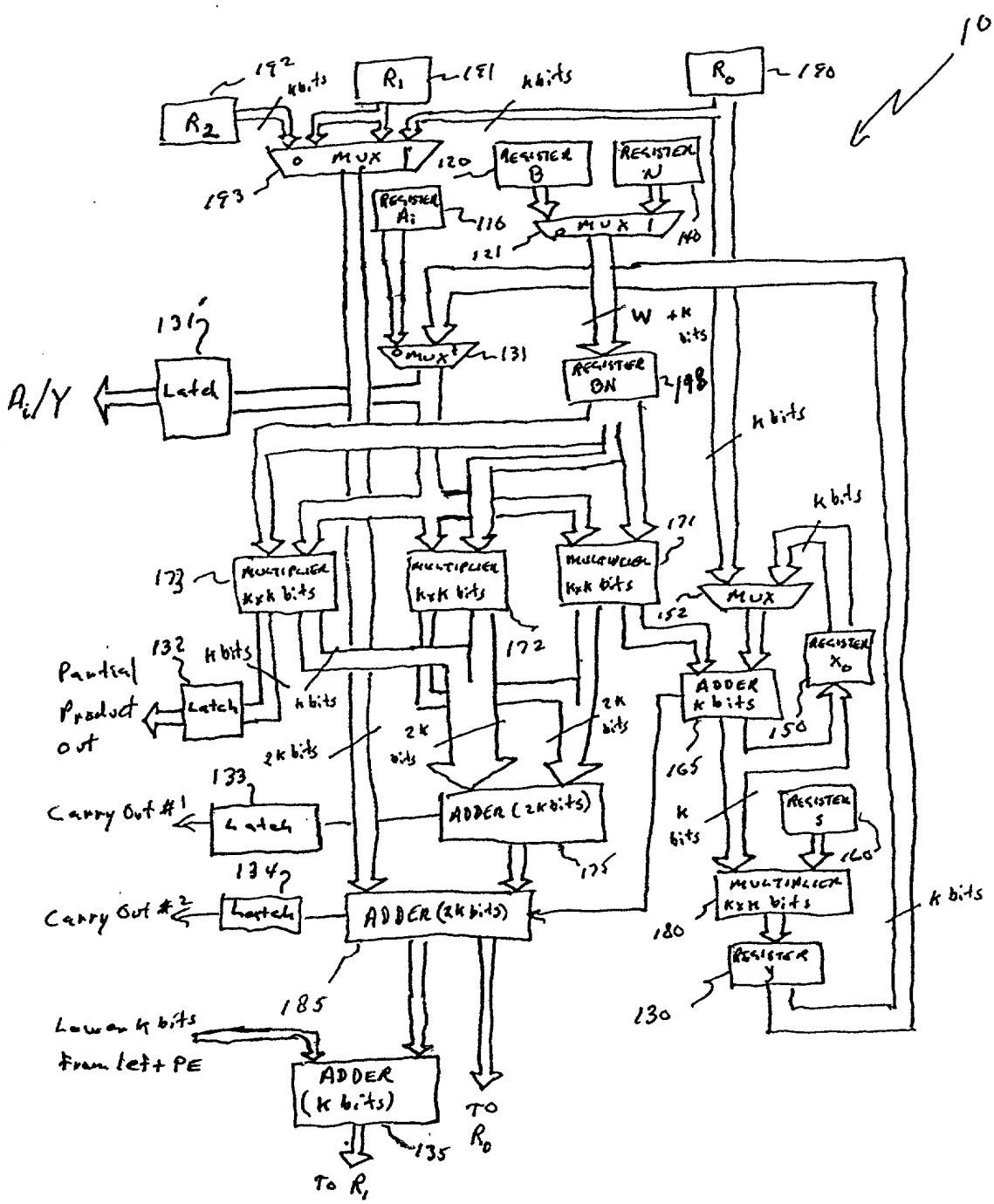

Figure 11

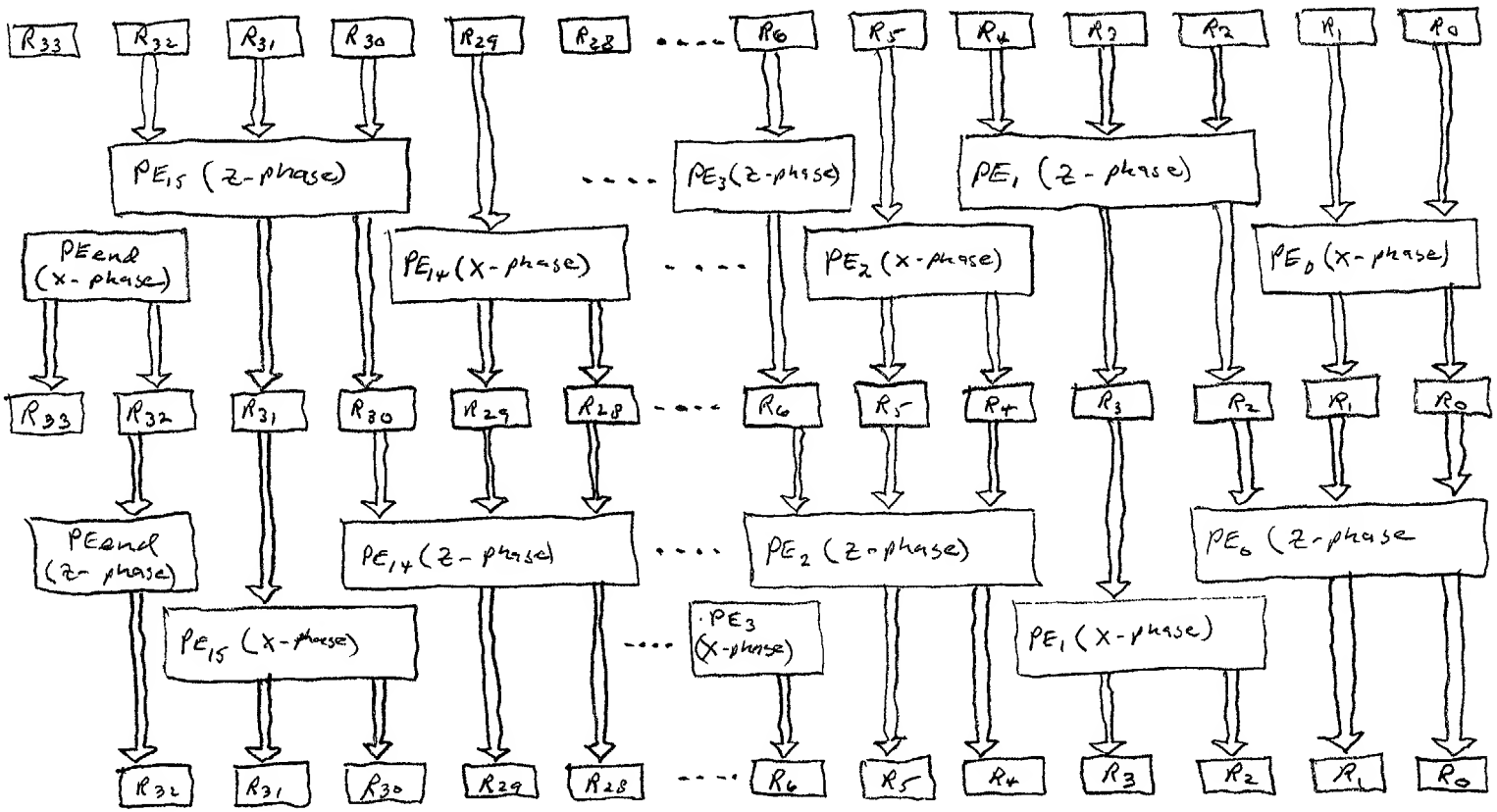

Figure 12

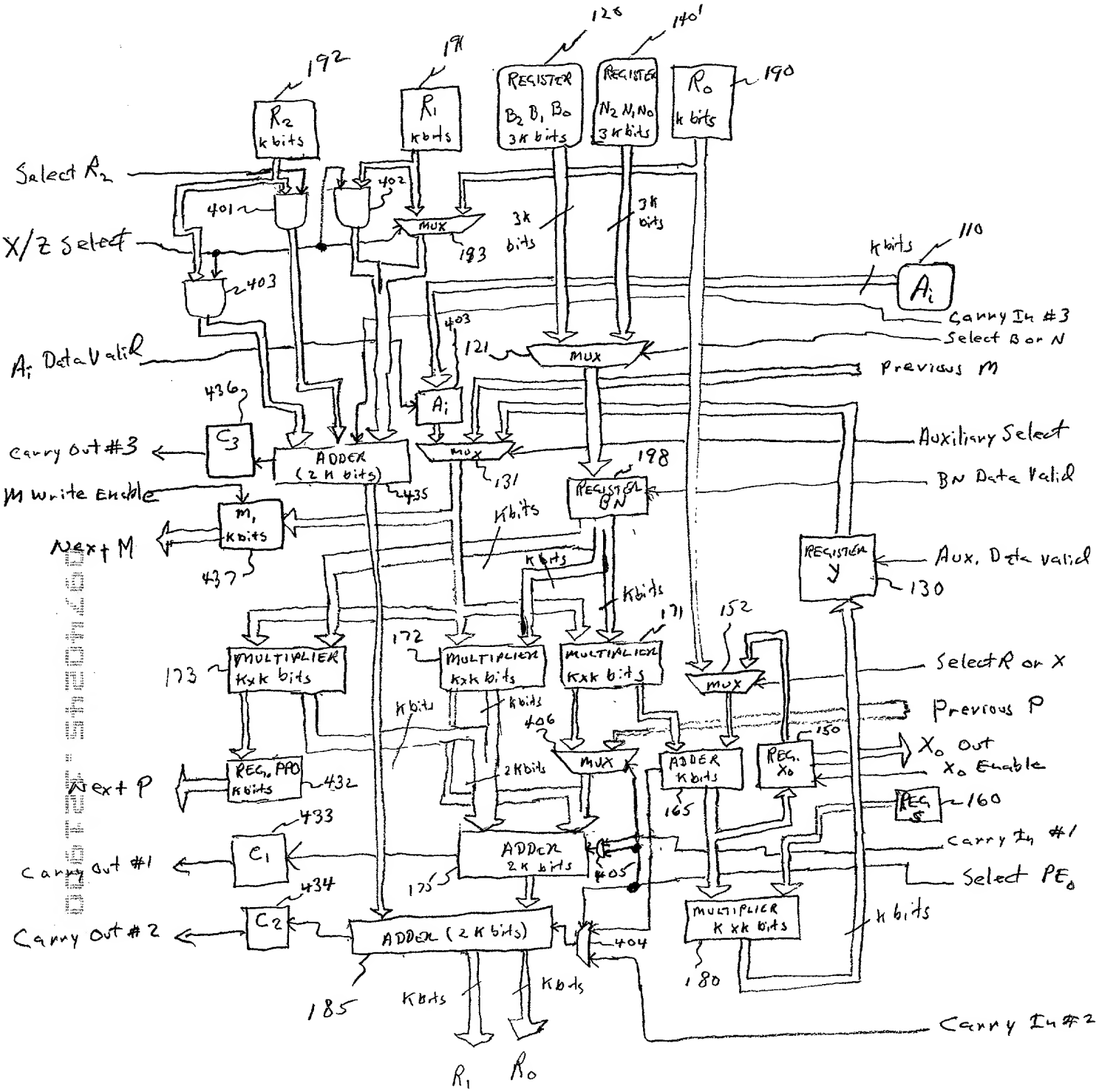
R_2 k bits
R_1 k bits
REGISTER $B_2 B_1 B_0$ 3k bits
REGISTER $N_2 N_1 N_0$ 3k bits
R_0 k bits
Select R_2
X/Z Select
A_i Data Valid
MUX
3k bits
A_i
k bits
Carry In #3
Select B or N
Previous M
Auxiliary Select
BN Data Valid
Aux. Data valid
Carry out #3
M write Enable
Next M
ADDER (2k bits)
C_3
M_1 k bits
REGISTER BN
REGISTER Y
MULTIPLIER k x k bits
Select R or X
Previous P
Next P
REG. P_{PO} k bits
X_0 out
X_0 Enable
REG. X_0
REG. S
ADDER k bits
ADDER 2k bits
C_1
Carry out #1
Carry In #1
Select PE_0
C_2
Carry out #2
ADDER (2k bits)
Carry In #2
R_1 R_0

Figure 13

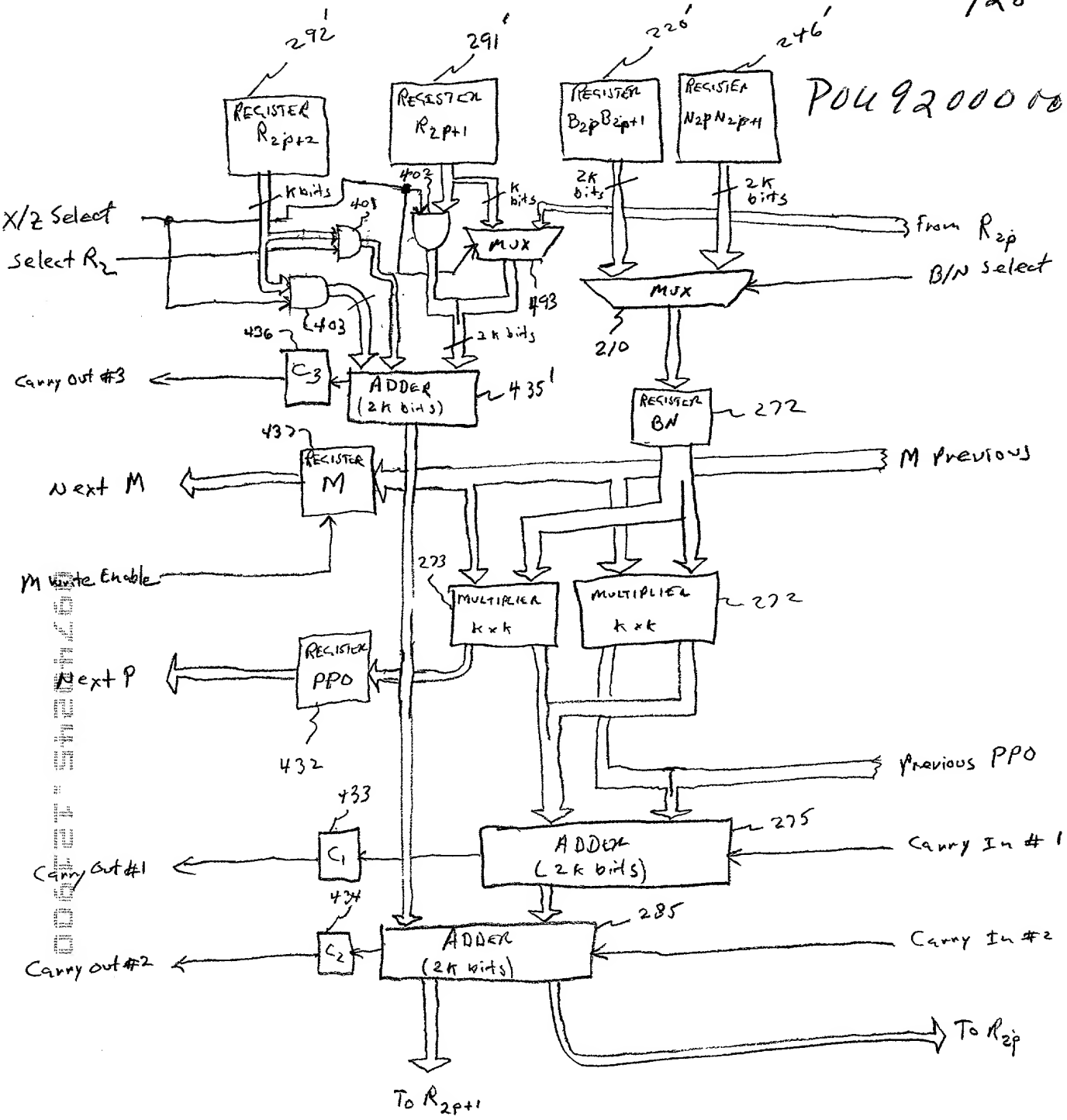

Figure 14

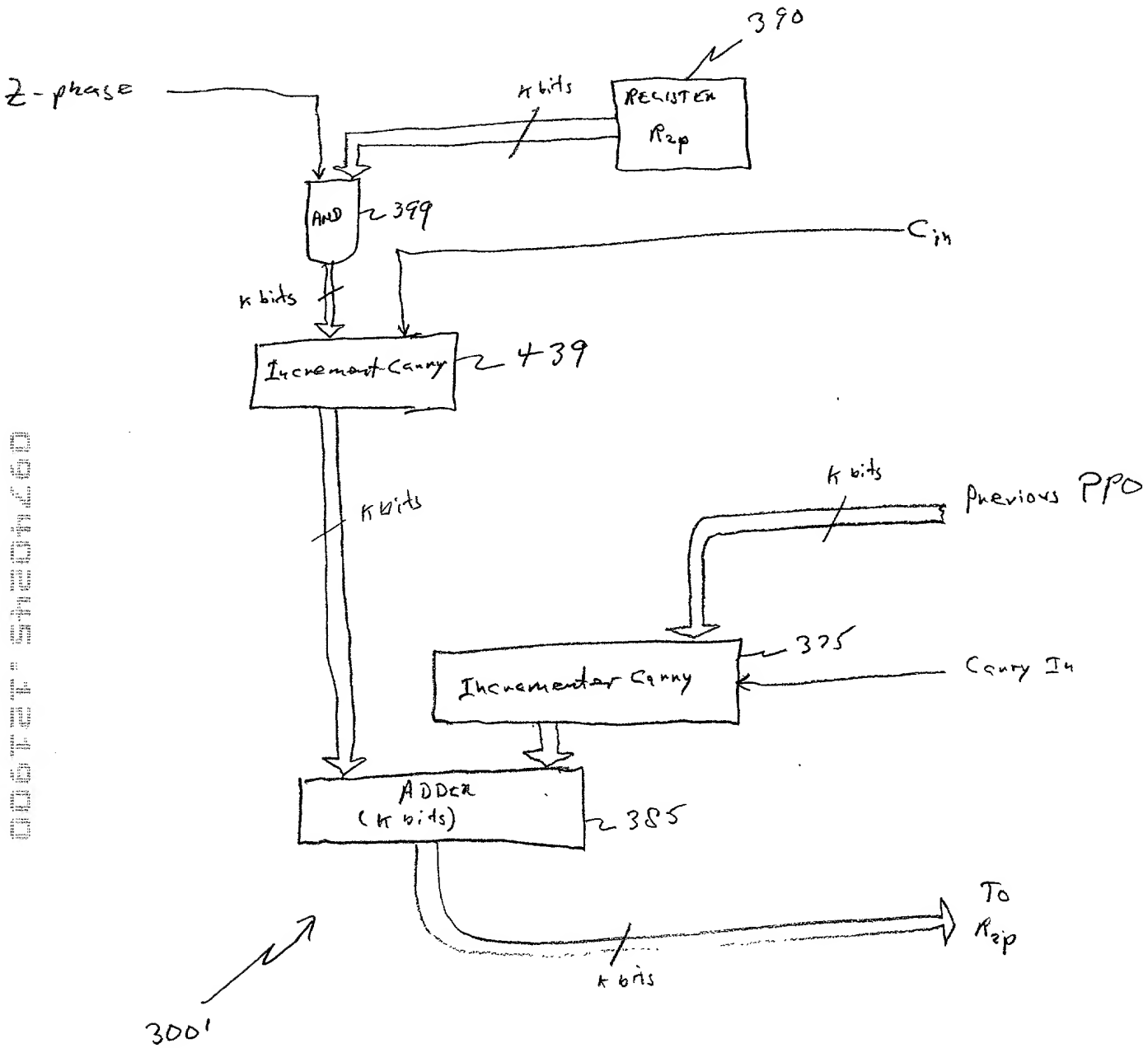
390
Z-phase
K bits
REGISTER
R_{zp}
AND
399
C_{in}
K bits
Increment Carry
439
K bits
K bits
Previous PPO
Incrementer Carry
375
Carry In
ADDER
(K bits)
385
To
R_{zp}
K bits
300'

Figure 15

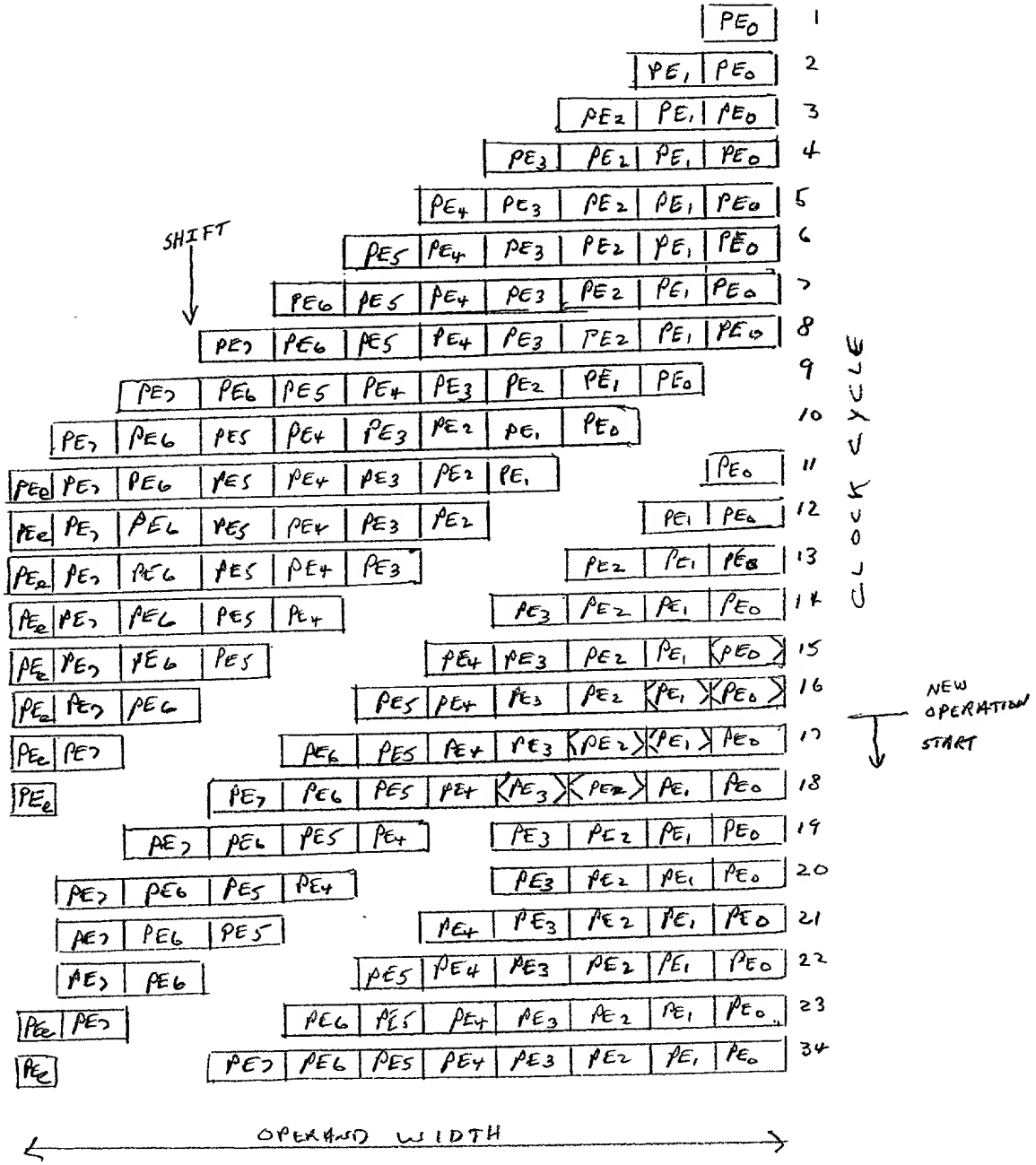

Figure 16

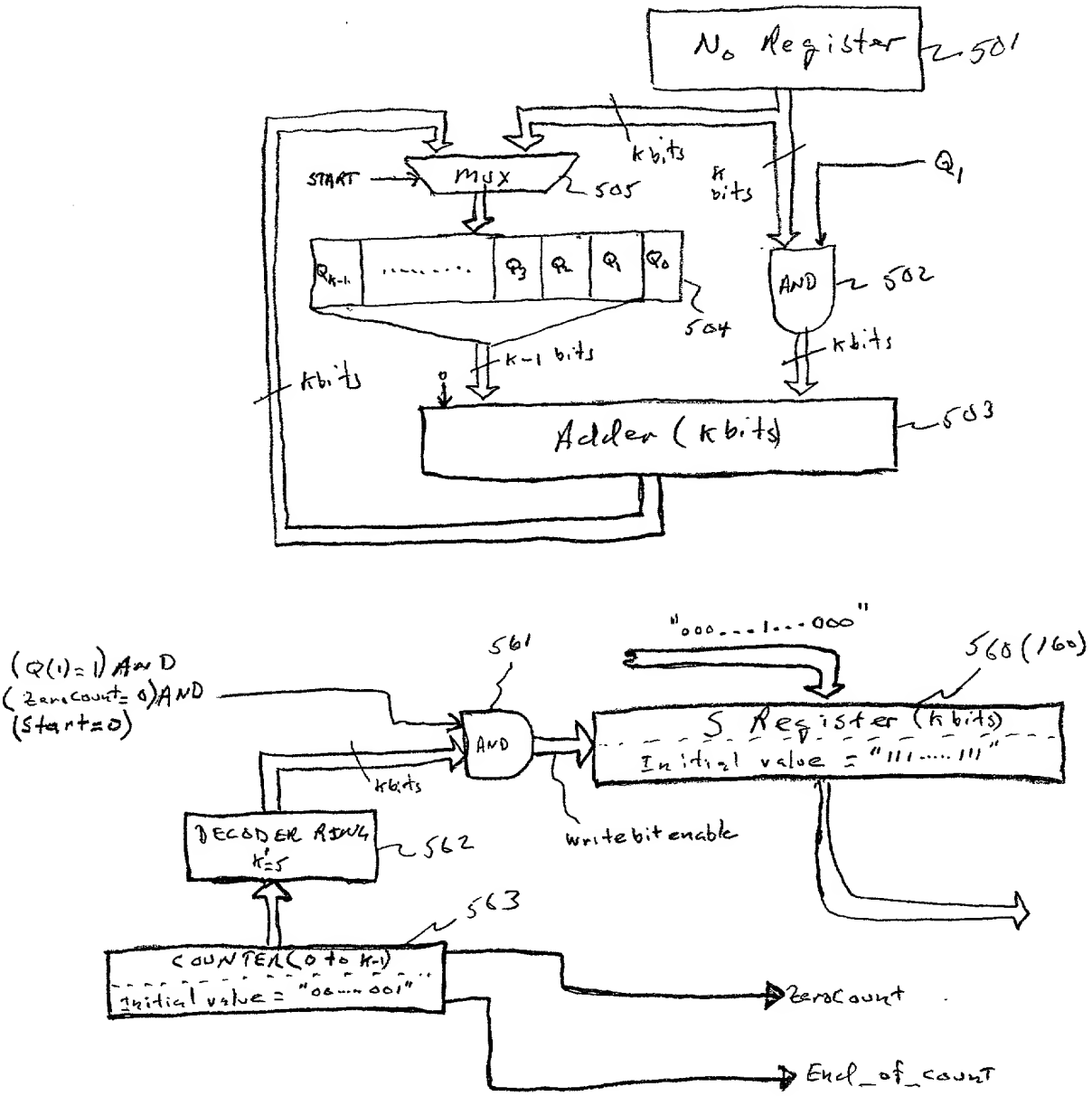

Figure 17

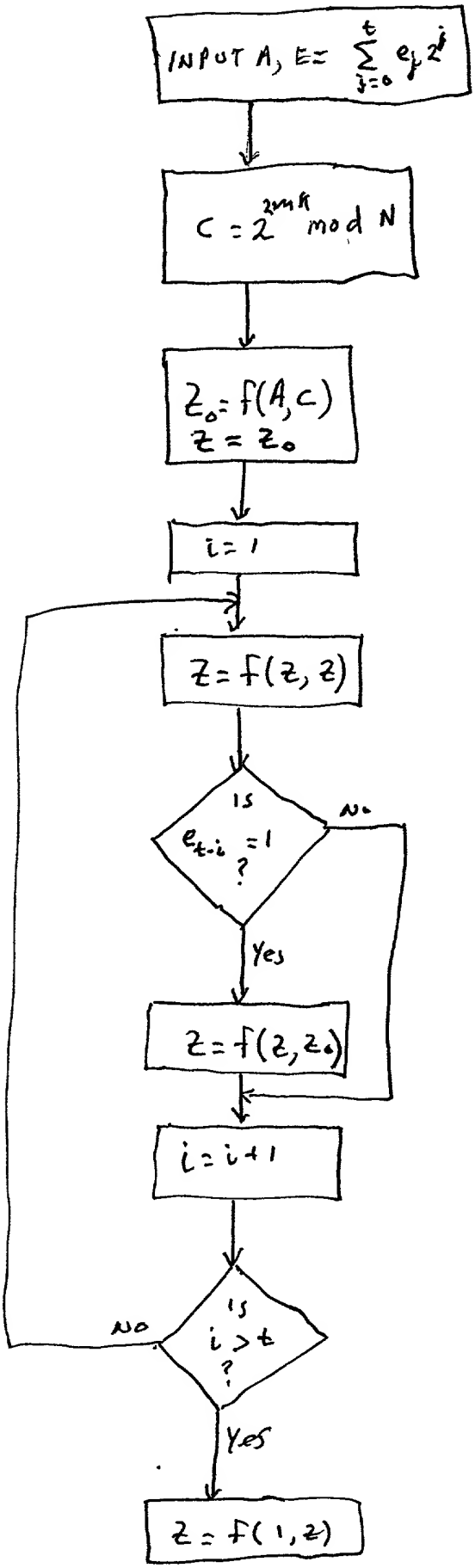

Figure 18

POU92000088US1

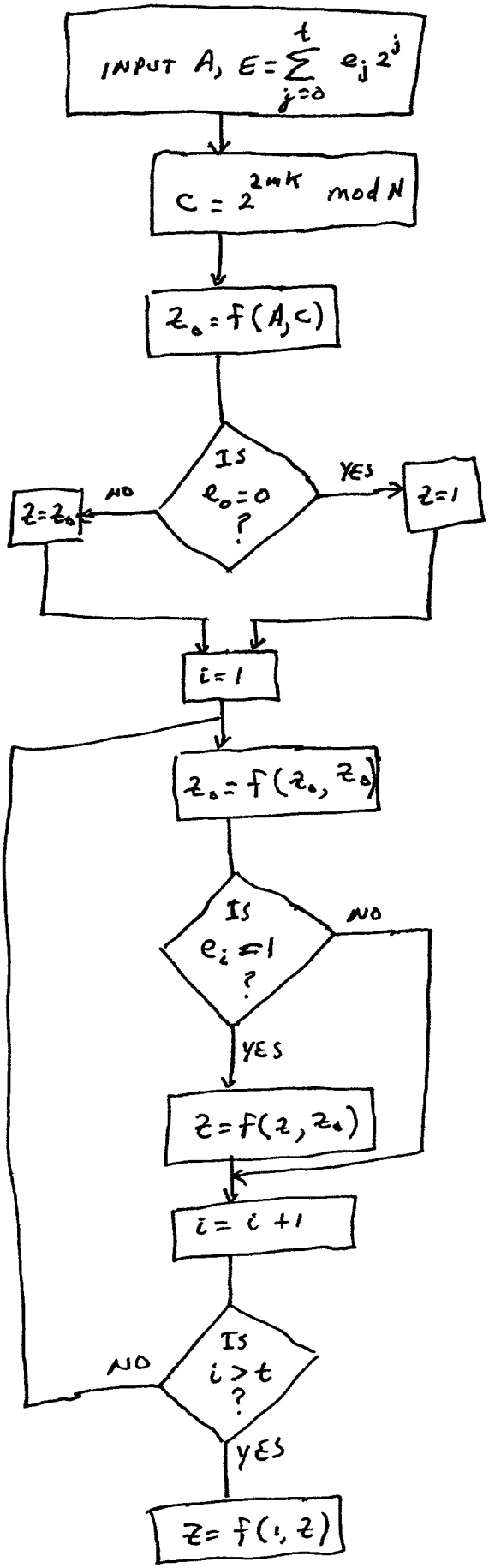

Figure 19

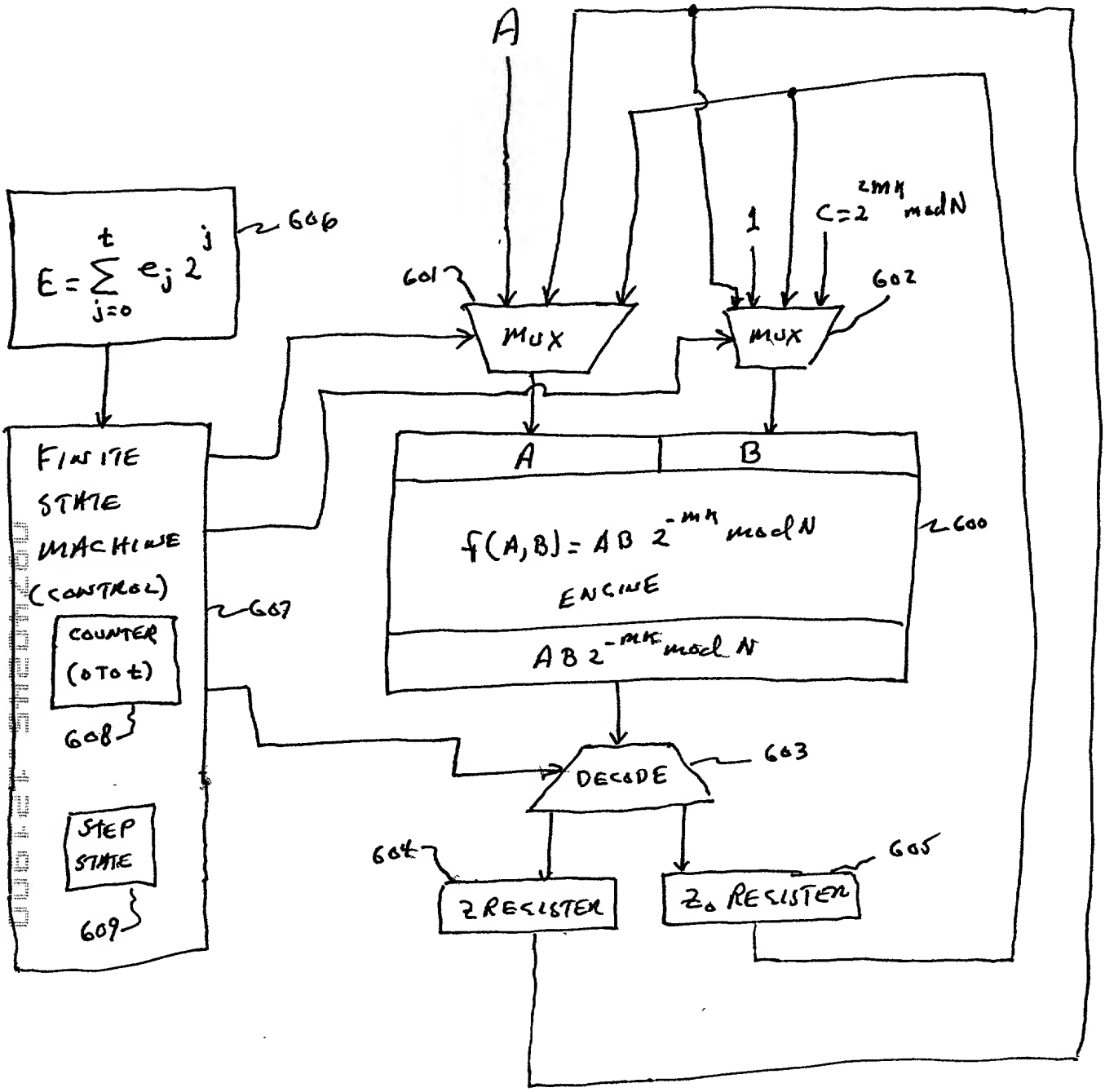
A
1
$C=2^{2mk} \bmod N$
$E=\sum_{j=0}^{t} e_j 2^j$
606
601
602
MUX
MUX
FINITE STATE MACHINE (CONTROL)
607
COUNTER (0 TO t)
608
STEP STATE
609
A
B
$f(A,B)=AB\,2^{-mk} \bmod N$
ENGINE
600
$AB\,2^{-mk} \bmod N$
DECODE
603
604
605
2 REGISTER
2_0 REGISTER

Figure 2d

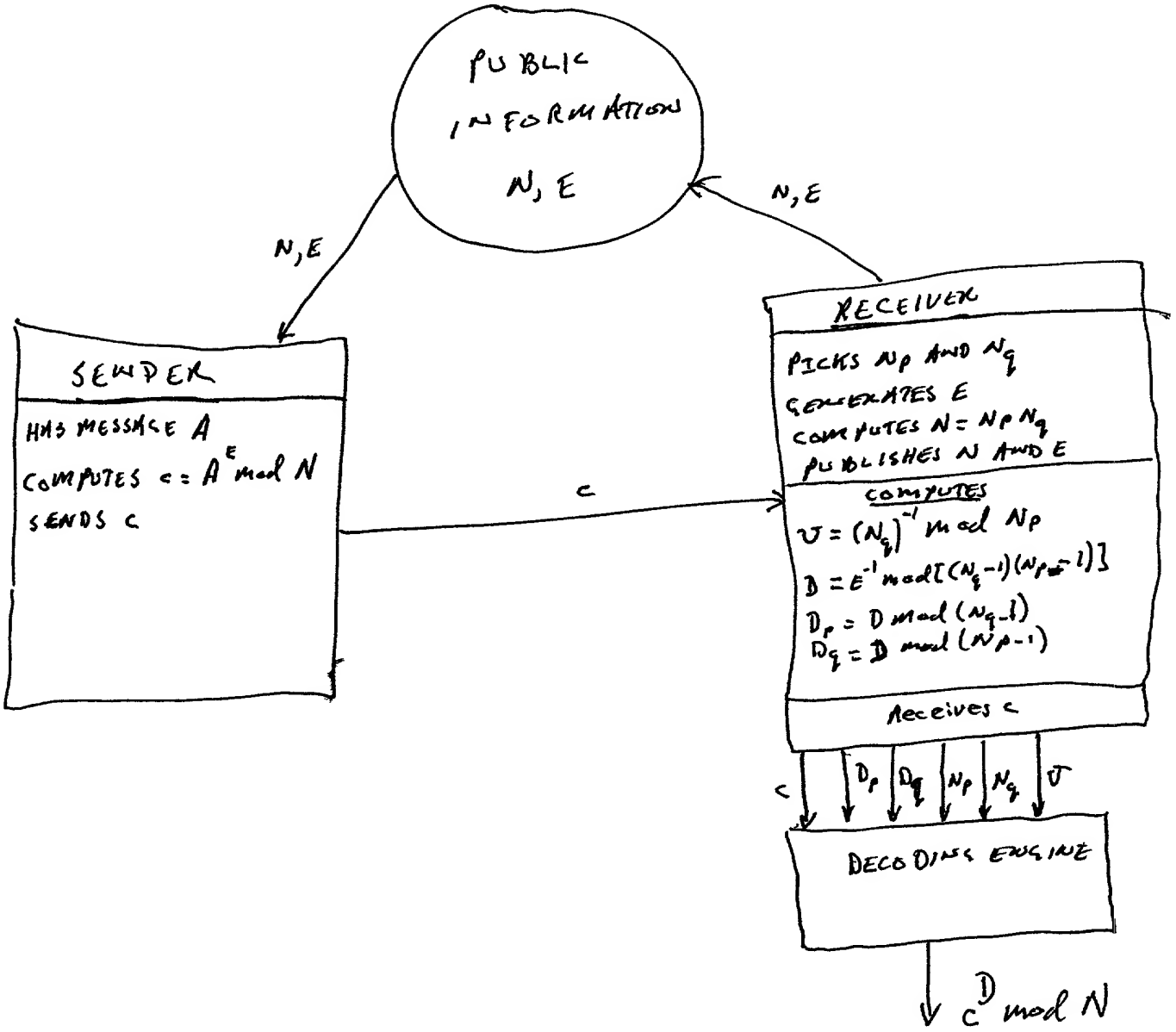
PUBLIC
INFORMATION
N, E
N, E
N, E
SENDER
HAS MESSAGE A
COMPUTES c = A^E mod N
SENDS c
c
RECEIVER
PICKS Np AND Nq
GENERATES E
COMPUTES N = Np Nq
PUBLISHES N AND E
COMPUTES
U = (Nq)^-1 mod Np
D = E^-1 mod [(Nq-1)(Np-1)]
Dp = D mod (Nq-1)
Dq = D mod (Np-1)
Receives c
c
Dp
Dq
Np
Nq
U
DECODING ENGINE
c^D mod N

Figure 21

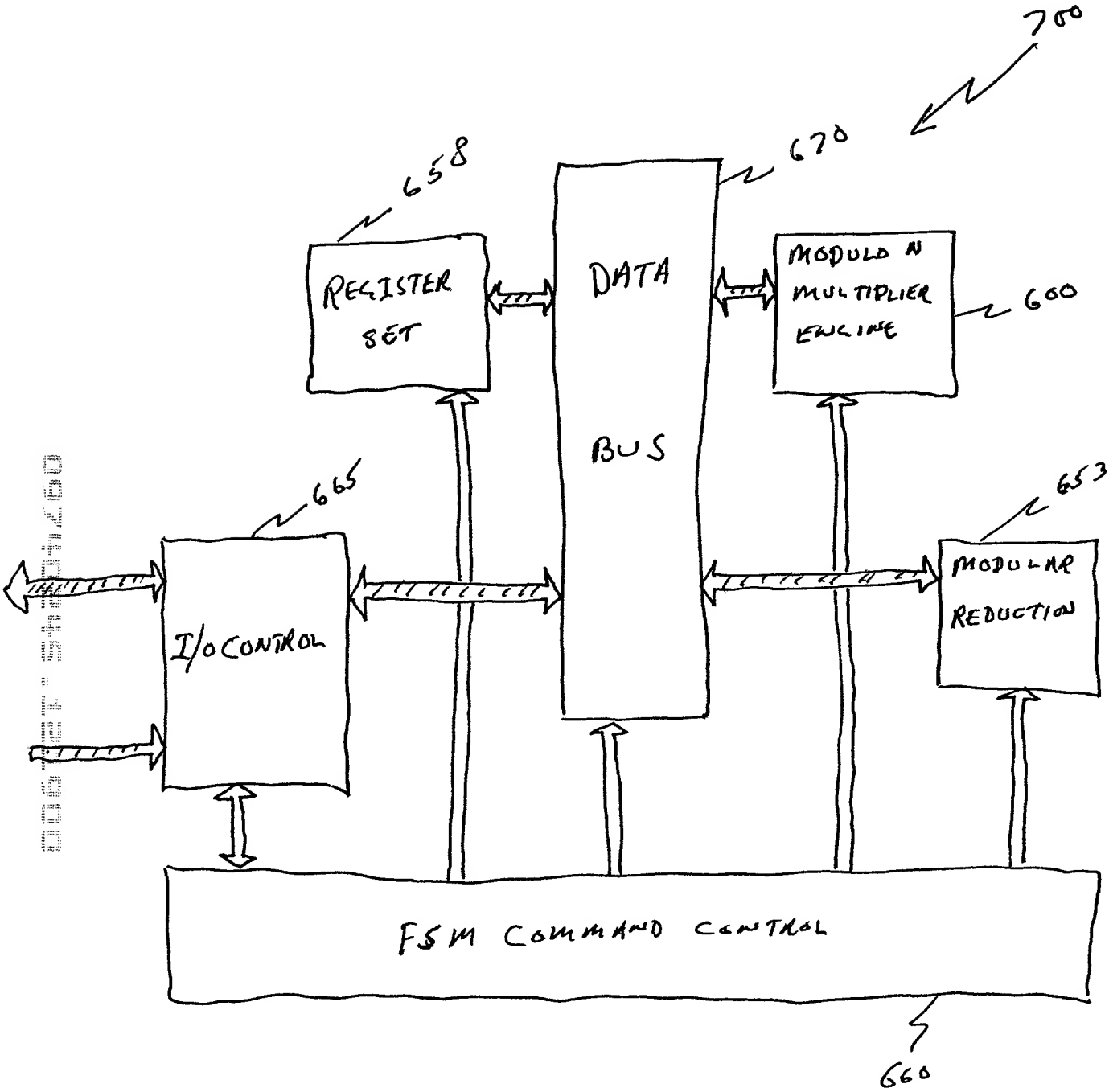
700
658
670
REGISTER SET
DATA BUS
MODULO N MULTIPLIER ENGINE
600
665
653
I/O CONTROL
MODULAR REDUCTION
FSM COMMAND CONTROL
660

Figure 22

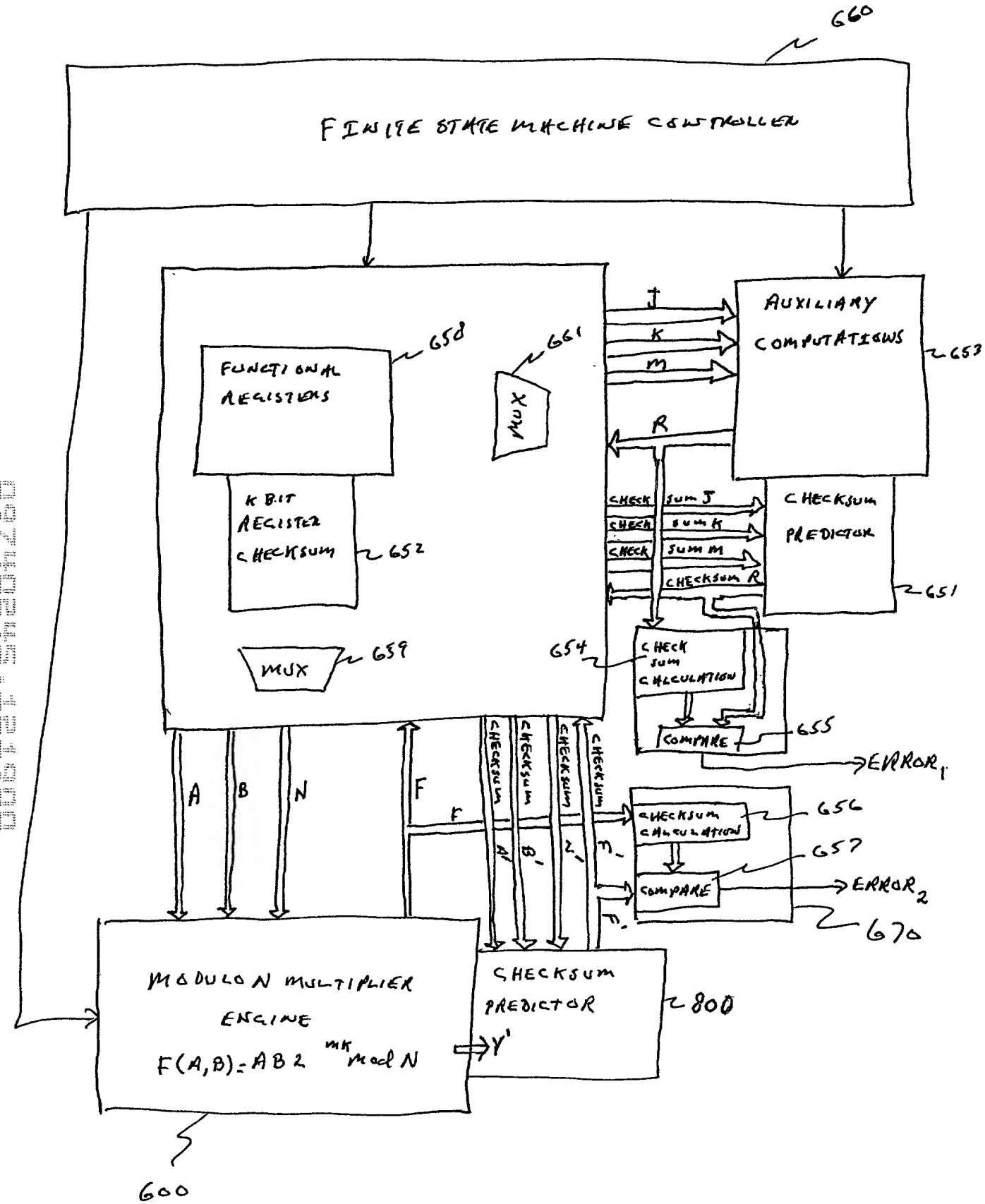
660
FINITE STATE MACHINE CONTROLLER
658
FUNCTIONAL REGISTERS
661
MUX
J
K
M
R
AUXILIARY COMPUTATIONS
653
K BIT REGISTER CHECKSUM
652
CHECK SUM J
CHECK SUM K
CHECK SUM M
CHECKSUM R
CHECKSUM PREDICTOR
651
MUX
659
654
CHECK SUM CALCULATION
COMPARE
655
ERROR1
A
B
N
F
F
CHECKSUM
CHECKSUM
CHECKSUM
CHECKSUM
A'
B'
N'
F'
F''
CHECKSUM CALCULATION
656
657
COMPARE
ERROR2
670
MODULO N MULTIPLIER ENGINE
F(A,B)=AB2^MK mod N
CHECKSUM PREDICTOR
800
Y'
600

Figure 23

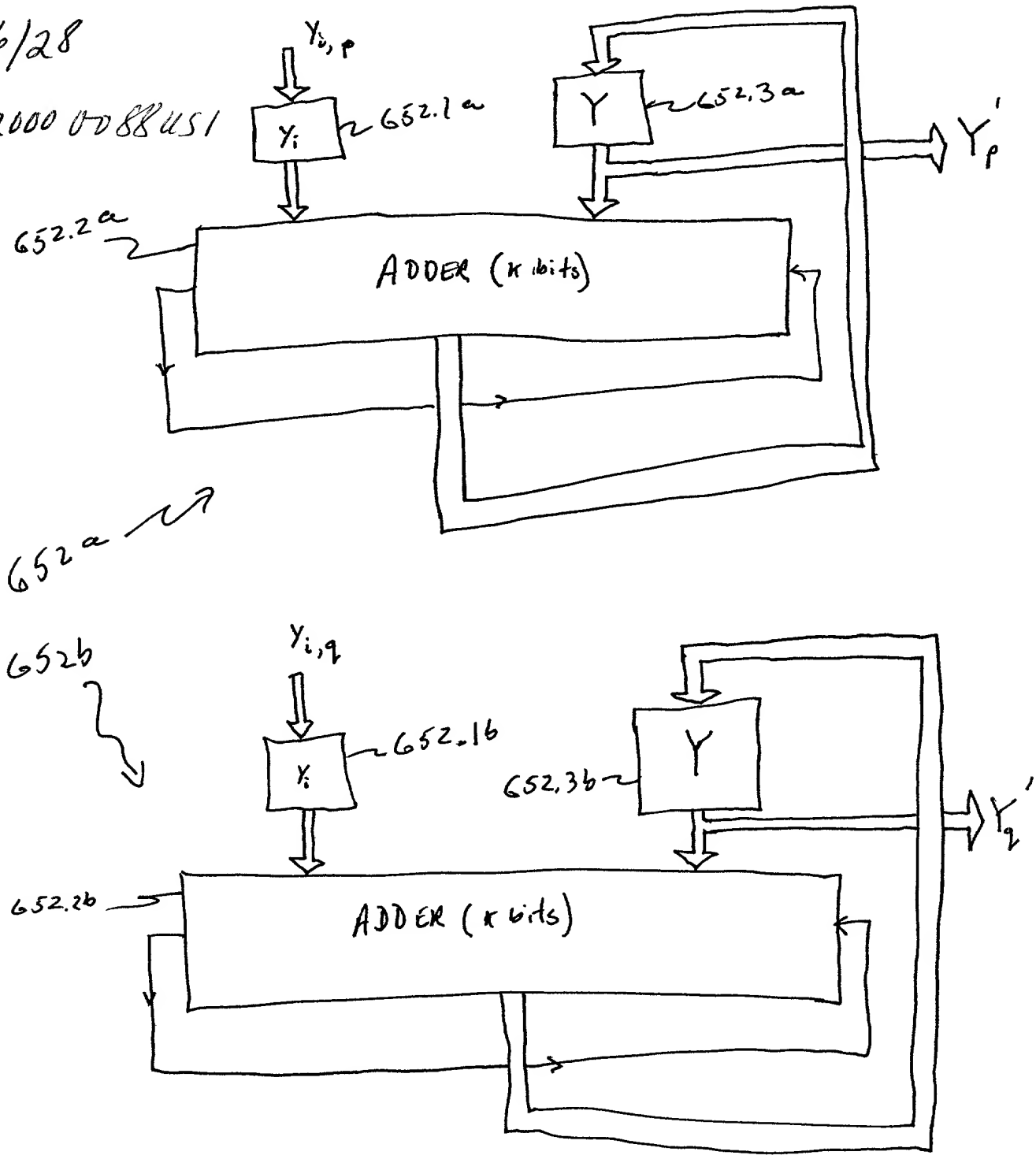
$Y_{i,p}$
Y_i
652.1a
Y
652.3a
Y_p'
652.2a
ADDER (x bits)
652a
652b
$Y_{i,q}$
Y_i
652.1b
652.3b
Y
Y_q'
652.2b
ADDER (x bits)

Figure 24

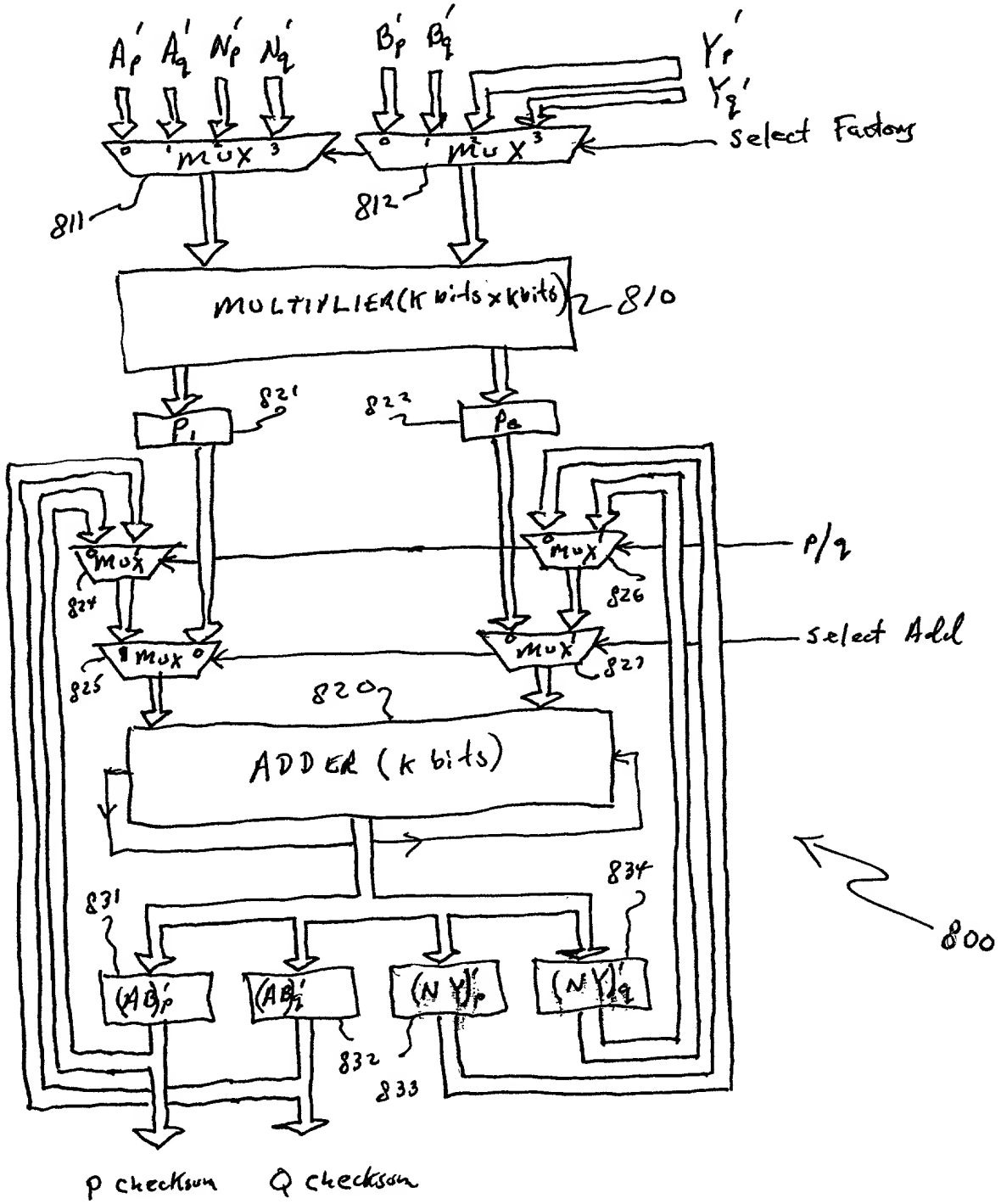
A'_p A'_q N'_p N'_q
B'_p B'_q
Y'_p
Y'_q
MUX 3
MUX 3
Select Factors
811
812
MULTIPLIER (K bits x K bits)
810
P_1
821
P_2
822
MUX
MUX
P/Q
824
826
MUX
MUX
Select Add
825
827
820
ADDER (K bits)
831
834
$(AB)'_p$
$(AB)'_q$
$(NY)'_p$
$(NY)'_q$
832
833
800
P checksum
Q checksum

Figure 25

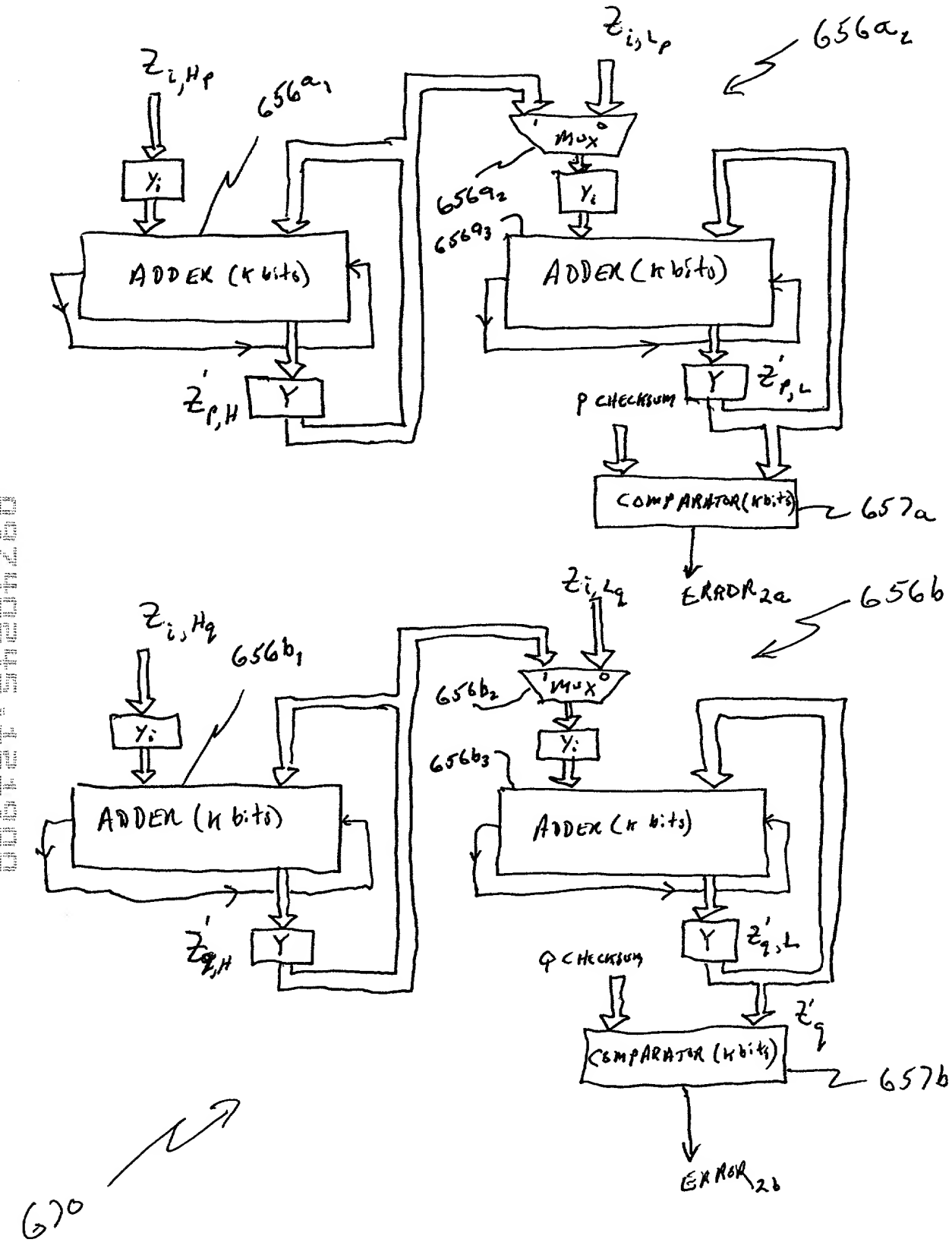
z_{i,H_p}
z_{i,L_p}
656a1
656a2
MUX
Y_i
ADDER (K bits)
$z'_{p,H}$
$z'_{p,L}$
p CHECKSUM
COMPARATOR (K bits)
657a
ERROR2a
z_{i,H_q}
z_{i,L_q}
656b1
656b2
656b3
$z'_{q,H}$
$z'_{q,L}$
q CHECKSUM
z'_q
657b
ERROR2b
600

Figure 26